

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-347616
 (43)Date of publication of application : 27.12.1993

(51)Int.CI.
 H04L 9/06
 H04L 9/14
 H04L 12/28

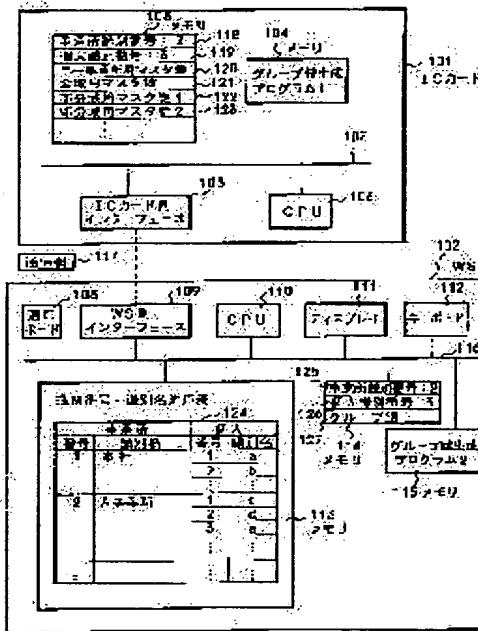
(21)Application number : 04-154733
 (71)Applicant : HITACHI LTD
 HITACHI CHUBU SOFTWARE LTD
 (22)Date of filing : 15.06.1992
 (72)Inventor : TAKARAGI KAZUO
 SUZAKI SEIICHI
 MATSUMOTO HIROSHI
 NAKAMURA TSUTOMU

(54) GROUP CIPHERING COMMUNICATION METHOD AND GROUP CIPHERING COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To attain group ciphering communication from one optional terminal to lots of optional terminals among plural terminals while the security is ensured.

CONSTITUTION: Plural secret numerals called as a master key in common to a prescribed partial set in an IC card 101 are stored in a memory 103 of the IC card, the IC card is inserted to a terminal to which communication is started at first to generate communication destination information is generated and sent to other terminal via a communication network 117. Moreover, based on communication destination information, one is selected from plural master keys and a group key is generated by using the selected master key and a communication message is ciphered or decoded by using the generated group key. A terminal being a communication destination receives communication destination information and selects one from the plural master keys based on the communication destination information and the group key is generated by using the selected master key and ciphering/decoding of the communication message is implemented by using the generated group key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-347616

(43)公開日 平成5年(1993)12月27日

(51)Int.Cl.⁵
H 04 L 9/06
9/14
12/28

識別記号

庁内整理番号

F I

技術表示箇所

7117-5K
8529-5K

H 04 L 9/02

11/00

Z

310 Z

審査請求 未請求 請求項の数14(全 16 頁)

(21)出願番号

特願平4-154733

(22)出願日

平成4年(1992)6月15日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71)出願人 000233457

日立中部ソフトウェア株式会社

愛知県名古屋市中区栄3丁目10番22号

(72)発明者 宝木 和夫

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72)発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74)代理人 弁理士 小川 勝男

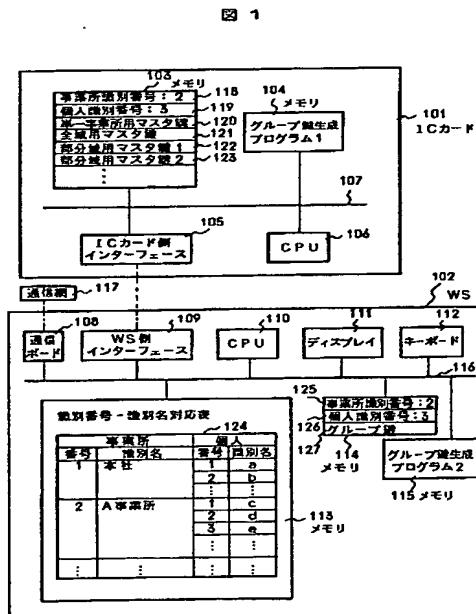
最終頁に続く

(54)【発明の名称】 グループ暗号通信方法およびグループ暗号通信システム

(57)【要約】 (修正有)

【目的】セキュリティ上の安全を確保しつつ、複数端末間で任意の1つの端末から任意の多数の端末へとグループ暗号通信ができるようにする。

【構成】ICカード101に、ICカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値をメモリ103に複数個格納し、最初に通信を開始する端末にICカードを差し込み、通信宛先情報を生成し通信網117を介し他の端末に送出する。また通信宛先情報に基づいて複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復号化を行う。通信宛先である端末においては、通信宛先情報を受け取り、該通信宛先情報に基づいて複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復号化を行う。



【特許請求の範囲】

【請求項1】複数のICカードと、ICカードの入出力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えた通信システムに適用するグループ暗号通信方法であって、

前記ICカードには、各ICカードを特定する個別の数値、およびICカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されており、

最初に通信を開始する端末においては、通信を行うべき相手先を特定する通信宛先情報を生成して、他の端末に送出するとともに、該通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受し、

通信宛先である端末においては、前記通信宛先情報を受け取り、該通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受することを特徴とするグループ暗号通信方法。

【請求項2】前記通信宛先情報は、通信を行うべき相手先を特定する情報と任意に選択された数値情報とからなり、かつ前記グループ鍵は、前記選択したマスタ鍵および前記通信宛先情報を用いて生成される請求項1に記載のグループ暗号通信方法。

【請求項3】前記グループ鍵は、ハッシュ関数を用いた計算によって生成される請求項1または2に記載のグループ暗号通信方法。

【請求項4】前記ICカードに格納されている個別の数値を用いて前記通信宛先情報を検査し、これにより該通信宛先情報が該ICカードの個別の数値を指定しているか否かを判定する請求項1ないし3に記載のグループ暗号通信方法。

【請求項5】前記通信宛先情報に基づいて前記複数のマスタ鍵から1つを選択し選択したマスタ鍵を用いてグループ鍵を生成する処理が、ICカード内部で実行される請求項1ないし4に記載のグループ暗号通信方法。

【請求項6】前記ICカードにはさらに、暗号関数およびICカードごとに異なる個別鍵と呼ばれる秘密数値が格納されており、該ICカードのマスタ鍵の更新は、マスタ鍵を個別鍵で暗号化したマスタ鍵暗号文を外部からICカードに入力し、該マスタ鍵暗号文を個別鍵と暗号関数を用いて復号化し、その結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより行う請求項1ないし5に記載のグループ暗号通信方法。

【請求項7】前記ICカードにはさらに、暗号関数およ

びICカードごとに異なる第1、第2、…の個別鍵と呼ばれる秘密数値が複数個格納されており、該ICカードのマスタ鍵の更新は、マスタ鍵を第1の個別鍵で暗号化したマスタ鍵分割暗号文を外部からICカードに入力

05 し、マスタ鍵を第2の個別鍵で暗号化したマスタ鍵分割暗号文を外部からICカードに入力し、…、このようにICカードに入力された複数のマスタ鍵分割暗号文を前記第1、第2、…の個別鍵と暗号関数を用いてそれぞれ復号化し、その結果に所定の演算を施した結果を前記マ

10 スタ鍵が書かれていた記憶領域上に上書きすることにより行う請求項1ないし5に記載のグループ暗号通信方法。

【請求項8】複数のICカードと、ICカードの入出力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えたグループ暗号通信システムであって、

前記ICカードには、各ICカードを特定する個別の数値、およびICカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されてい

20 るとともに、

前記ICカードが差し込まれた端末は、通信を行うべき相手先を特定する通信宛先情報を生成し出力する手段と、自端末が生成したまたは外部端末が生成した通信宛先情報に基づいて自端末に差し込まれているICカードに

25 格納されている前記複数のマスタ鍵から1つを選択する手段と、選択したマスタ鍵を用いてグループ鍵を生成する手段と、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行う手段とを備えることを特徴とするグループ暗号通信システム。

30 【請求項9】前記通信宛先情報は、通信を行うべき相手先を特定する情報と任意に選択された数値情報とからなり、かつ前記グループ鍵を生成する手段は、前記選択したマスタ鍵および前記通信宛先情報を用いてグループ鍵を生成する請求項8に記載のグループ暗号通信システム。

35 【請求項10】前記グループ鍵を生成する手段は、ハッシュ関数を用いた計算によってグループ鍵を生成する請求項8または9に記載のグループ暗号通信システム。

【請求項11】前記ICカードに格納されている個別の数値を用いて前記通信宛先情報を検査し、これにより該通信宛先情報が該ICカードの個別の数値を指定しているか否かを判定する請求項8ないし10に記載のグループ暗号通信システム。

40 【請求項12】前記通信宛先情報に基づいて複数のマスタ鍵から1つを選択する手段と、選択したマスタ鍵を用いてグループ鍵を生成する手段とが、前記ICカード内部に設けられている請求項8ないし11に記載のグループ暗号通信システム。

45 【請求項13】前記ICカードにはさらに、暗号関数およびICカードごとに異なる個別鍵と呼ばれる秘密数値

が格納されており、

該 I C カードは、マスタ鍵を個別鍵で暗号化したマスタ鍵暗号文を外部から入力し、該マスタ鍵暗号文を個別鍵と暗号関数を用いて復号化し、その結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより、マスタ鍵の更新を行う手段を備えた請求項 8 ないし 12 に記載のグループ暗号方法。

【請求項 14】前記 I C カードにはさらに、暗号関数および I C カードごとに異なる第 1, 第 2, … の個別鍵と呼ばれる秘密数値が複数個格納されており、

該 I C カードは、マスタ鍵を第 1 の個別鍵で暗号化したマスタ鍵分割暗号文を外部から入力し、マスタ鍵を第 2 の個別鍵で暗号化したマスタ鍵分割暗号文を外部から I C カードに入力し、…、このように I C カードに入力された複数のマスタ鍵分割暗号文を前記第 1, 第 2, … の個別鍵と暗号関数を用いてそれぞれ復号化し、その結果に所定の演算を施した結果を前記マスタ鍵が書かれていた記憶領域上に上書きすることにより、マスタ鍵の更新を行う手段を備えた請求項 8 ないし 12 に記載のグループ暗号方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、通信メッセージを暗号化して送受する通信方法およびシステムに関する。

【0002】

【従来の技術】近年、情報および通信の技術の進展によって、通信網を使って種々の情報を高速かつ安価にやり

通信宛先情報=事業所番号 1 || 配布リスト 1 || 乱数 1 || 鍵情報 1 ||
事業所番号 2 || 配布リスト 2 || 乱数 2 || 鍵情報 2 ||

ここに、|| はデータのつなぎ合わせを示す。

【0009】この後、WS 902 は I C カードのメモリ 903 から予め読み取っていた事業所識別番号 925 の数値「2」と個人識別番号 926 の数値「3」に基づいて、自 WS が通信宛先の対象に含まれているかどうかを検査する。例えば、上記の通信宛先情報のうち、事業所番号 1 が数値「2」であり、配布リスト 1 がビット列「00…0101」であったとする。この例では、WS 902 内のメモリ 914 に格納されている事業所識別番号 925 の数値は「2」で上記通信宛先情報の事業所番号 1 と一致している。また、WS 902 内のメモリ 914 に格納されている個人識別番号 926 の数値は「3」であるので、この数値「3」でポイントされる配布リスト 1 の下から 3 番目のビットを参照すると、それは「1」になっている。そこで、事業所識別番号 925 (数値は「2」) と個人識別番号 926 (数値は「3」) が該通信宛先情報に含まれている、と判定する。

とりすることができるようになってきた。通信衛星やローカルエリアネットワークを使う場合、1 つの情報を送信すると多数の端末で同時に受信することができる。すなわち、同報通信を簡単に実現できるという特徴がある。

05 【0003】ところで、通信衛星やローカルエリアネットワークを使って同報通信を行う場合、送出された電気または電波信号はどの端末でも受信可能であり、そのままでは秘密にしたい情報を限定された相手にだけ伝えるような限定的通信を行うことはできない。

10 【0004】通信衛星やローカルエリアネットワークを使って同報通信を行う場合に、限定された相手にだけ情報を伝え、それ以外の相手には情報を秘密にするための一方法が、例えば、宝木、福澤、中村、「カードによる 15 セキュリティ」、情報社会における通信網の安全・信頼性シンポジウム、電子情報通信学会、1991年8月19日などに示されている。

15 【0005】図 9 を用いて、上記従来例で開示されている方法を説明する。

20 【0006】図 9 は、従来の通信システムにおける受信側のワークステーション (WS) 902、および I C カード 901 を示している。

25 【0007】先ず、WS 902 は通信網 917 経由で通信宛先情報を受け取る。通信宛先情報は、下記のような情報を含む。

【0008】

【0010】次に、WS 902 は、該当する通信宛先情報「事業所番号 1 || 配布リスト 1 || 乱数 1 || 鍵情報 1 ||」35 を I C カード 901 に送信する。そして、I C カード 901 内でも、事業所識別番号 918 (数値は「2」) と個人識別番号 919 (数値は「3」) を使って同様の検査を行う。検査結果が「含まれている」であれば、単一事業所用マスタ鍵 920 を使って次の計算を行う。

40 【0011】ワーク鍵 ← H(単一事業所用マスタ鍵、事業所番号 1 || 配布リスト 1 || 乱数 1)
グループ鍵 ← D(ワーク鍵、鍵情報 1)
ここに、H(I, M) は初期値を I、入力データを M とするハッシュ関数 H による出力 (ハッシュトータル) である。また、D(K, M) は鍵を K、入力データを M とする復号化関数 D による出力である。

45 【0012】I C カード 901 は、以上のようにして算出したグループ鍵を WS 902 に渡す。WS 902 は、このグループ鍵 (メモリ 914 内のグループ鍵の記憶領域 927 に格納される) を使って、通信網 917 から送

信されてくる暗号メッセージを復号化する。

【0013】以上により、ICカード901が差し込まれているWS902において、自WSが通信宛先情報に含まれていることを判別し、鍵を生成して、暗号メッセージを復号化することができる。

【0014】同様に他のWSにおいても、通信宛先情報に含まれる事業所識別番号と個人識別番号を持つICカードが差し込まれていれば、グループ鍵を生成する処理が行われ、その結果通信網917から送信されてくる暗号メッセージを復号化できる状態となる。

【0015】このようにして、1つの送信元から多数の受信先への一对多数の暗号通信を行うことができる。

【0016】

【発明が解決しようとする課題】ところで、上記従来例において、一对多数通信のうちの多数の側の1つが送信側になることはできなかった。つまり、受信側のICカードおよびWSが上記通信宛先情報を生成することはできなかった。これは、受信側のICカードが該ICカードが属する事業所にしか通用しない单一事業所用マスタ鍵を1つしか持たないためである。

【0017】本発明の目的は、上述の従来例における問題点に鑑み、セキュリティ上の安全を確保しつつ、複数端末間で任意の1つの端末から任意の多数の端末へとグループ暗号通信ができるようにすることにある。

【0018】

【課題を解決するための手段】上記課題を解決するため、本発明は、複数のICカードと、ICカードの出入力インターフェースを有する複数の通信端末と、それらの通信端末を結ぶ通信網とを備えた通信システムに適用するグループ暗号通信方法およびシステムであって、前記ICカードには、各ICカードを特定する個別の数値、およびICカードの所定の部分集合において共通であるマスタ鍵と呼ばれる秘密数値が複数個格納されており、最初に通信を開始する端末においては、通信を行るべき相手先を特定する通信宛先情報を生成して、他の端末に送出するとともに、該通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受し、通信宛先である端末においては、前記通信宛先情報を受け取り、該通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信メッセージの暗号化および復合化を行って、通信メッセージを授受するようにしている。

【0019】ICカード毎の個別の数値は、ICカードに入力される通信宛先情報と呼ばれるデータ列のある特定位置を検査するための、検査位置指定用のポイントと

して用いるとよい。この検査によりそのICカードが差し込まれた端末が通信宛先になっているのか否かが分かる。通信宛先になっているときは、通信宛先情報から複数のマスタ鍵のうちの1つを選択する。ICカードのマ5
05
スタ鍵は、この通信システム内の端末から正当にアクセスされたとき以外は読出しができないようにしておくとよい。

【0020】グループ鍵は、選択された秘密数値であるマスタ鍵と通信宛先情報を含むデータを入力としてハッ

10
10
シュ関数による計算を行って求めるとよい。

【0021】さらにICカードに、暗号関数とICカード外部に出ないICカードごとに異なる個別鍵と呼ばれる秘密数値を保持し、ICカードに入力されるマスタ鍵暗号文と呼ばれるデータに対して、該個別鍵と暗号関数15
15
を用いて、復号化計算を行い、その計算結果を前記マスタ鍵が書かれていたエリア上に上書きすることにより、マスタ鍵の更新を行うようにしてもよい。

【0022】

【作用】最初に通信を開始する端末は、通信を行すべき20
20
相手先を特定する通信宛先情報を生成して、他の端末に送出する。そして、通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信

25
25
メッセージの暗号化および復合化を行って、通信メッセージを授受する。一方、通信宛先である端末は、前記通信宛先情報を受取り、該通信宛先情報に基づいて自端末に差し込まれているICカードに格納されている前記複数のマスタ鍵から1つを選択し、選択したマスタ鍵を用いてグループ鍵を生成し、生成したグループ鍵を用いて通信

30
30
メッセージの暗号化および復合化を行って、通信メッセージを授受する。結果、各端末において同一のマスタ鍵を用いてグループ鍵が生成される。したがって、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。

【0023】通信中の事業所以外の事業所に属するIC40
40
カードの中身が万一漏洩したとしても、該事業所の間では特有のマスタ鍵が用いられるので、それらの事業所の間では通信の安全性に影響を与えることはない。複数事業所にまたがり鍵共有を行おうとする場合に、もし適当な部分域用マスタ鍵がICカード内になかったときには、全域に有効なマスタ鍵を用いればよい。この場合、すべてのICカードの中身が漏洩していなければ、安全

45
45
である。

【0024】上述の個別鍵を用いて暗号化したマスタ鍵暗号文を入力してマスタ鍵を更新する方式を用いれば、マスタ鍵漏洩等の事情によりマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。

【0025】また、複数の個別鍵を用いて暗号化したマスタ鍵分割暗号文を入力してマスタ鍵を更新する方式では、マスタ鍵が複数の鍵センタの共同作業により生成されることになる。したがって、複数の鍵センタが結託しない限り、マスタ鍵が鍵センタの単独作業により知られることはない。よって、通信当事者間のプライバシーを鍵センタに対しても保護することができる。

【0026】

【実施例】以下、図面を用いて、本発明の実施例を説明する。

【0027】図10は、本発明のグループ暗号方法および装置を適用した暗号通信システムを示す。この暗号通信システムは、ICカードの入出力インターフェースを有する5つの通信端末1002、1004、1006、1008、1010、およびそれらを結ぶ通信網1001を備えている。通信端末1002、1004、1006、1008、1010には、それぞれICカード1003、1005、1007、1009、1011が差し込まれている。

【0028】各ICカードには、ICカード別の個別の数値1012、1016、1019、1023、1026が記憶されている。この個別数値(x, y)の、xは事業所番号、yはその事業所内の個人番号を示す。ここでは事業所番号「1」が本社、「2」がA事業所を表すものとする。ICカード1003の個別数値1012は(1, 1)であるからこのカードは本社のaさん用、ICカード1005の個別数値1016は(1, 2)であるからこのカードは本社のbさん用、ICカード1007の個別数値1019は(2, 1)であるからこのカードはA事業所のcさん用、ICカード1009の個別数値1023は(2, 2)であるからこのカードはA事業所のdさん用、ICカード1011の個別数値1026は(2, 3)であるからこのカードはA事業所のeさん用、というようになる。

【0029】さらに、各ICカードには、ICカードから外部への読み出しが禁止されているマスタ鍵と呼ばれる秘密数値が格納されている。このうち、本社用マスタ鍵1013、1017は、本社のaさん用カード1003とbさん用カード1005で共通である。また、A事業所用マスタ鍵1020、1024、1027は、A事業所のcさん用カード1007、dさん用カード1009およびeさん用カード1011で共通である。全域用マスタ鍵1015、1018、1022、1025、1029は、5枚のICカード1003、1005、1007、1009、1011すべてで共通である。

【0030】図1は、図10のうちA事業所のeさん用カード1011と通信端末1010の詳細を示す。図1において、ICカード1011(図10の1011)は、ICカード側インターフェース105およびWS側インターフェース109を経由して、ワークステーション

(WS)102とデータのやりとりを行う。WS102は、通信ボード108を経由して通信網117とデータのやりとりを行う。

【0031】ICカード101では、メモリ104内の

- 05 グループ鍵生成プログラム1にしたがってCPU106が動作する。メモリ103内の事業所識別番号118(図10の個別数値1026の第1番目)の数値は「2」で、個人識別番号119(図10の個別数値1026の第2番目)の数値は「3」が格納されており、該10 ICカード101の所有者は事業所番号「2」の事業所(A事業所)に属する番号「3」の個人であることを示す。より具体的には、メモリ113に格納されている識別番号-識別名対応表124により、該ICカード101の所有者はA事業所のEさんであることが分かる。單15一事業所用マスタ鍵120(図10の1017)、全域用マスタ鍵121(図10の1029)、部分域用マスタ鍵122、123(図10の1028)、…はそれぞれ64ビット長のランダムなデータである。

- 【0032】WS102では、メモリ115内のグループ鍵生成プログラム2にしたがってCPU110が動作する。メモリ113内の識別番号-識別名対応表124は、事業所番号「1」は本社であることを示し、本社内の個人番号「1」はaさん、個人番号「2」はbさん、…であることを示す。同様に、事業所番号「2」はA事業所であることを示し、A事業所内の個人番号「1」はcさん、個人番号「2」はdさん、個人番号「3」はeさん、…であることを示す。メモリ114は、このWS102に差し込まれたICカード101の事業所識別番号118および個人識別番号119を読み出して格納する領域125、126を有する。ここでは事業所識別番号118が「2」、個人識別番号119が「3」であるので、事業所識別番号125は「2」、個人識別番号126は「3」になっている。また、メモリ114は、グループ鍵の生成結果を格納する領域127を有する。

- 35 【0033】その他、WS102には、WSの操作員に入出力手段を提供するディスプレイ111、およびキーボード112などを備えている。

- 【0034】上述したように、各ICカードはその所有者に固有の事業所識別番号および個人識別番号(図10では個別数値と呼んでいる)を格納している。ICカードを通信網117内のいずれかの端末に差し込むことにより、その所有者は通信網117を介して他の人と通信し合える環境となる。

- 【0035】以下、通信網の誰かが複数の通信相手を任意に指定して暗号通信を行おうとする場合に、それらの通信相手と暗号鍵を共有し合う方式について説明する。

- 【0036】図2は、メモリ115に格納されているグループ鍵生成プログラム2の動作を説明するためのフローチャートである。まずステップ201で処理が開始され、ステップ202で、操作員はキーボード112より

最初に鍵生成を行うことを示すコマンド、もしくは他の通信相手の後で鍵生成を行うことを示すコマンドを入力する。ステップ203では、もし前後のコマンドであればステップ204へ、もし後者のコマンドであればステップ211へ、それぞれ分岐する。最初に鍵生成を行うということは、この端末から他の端末に向けて最初に通信を開始するということであり、そのために最初に鍵生成を行う。他の通信相手の後で鍵生成を行うということは、他の通信相手が最初に鍵生成を行って通信を開始しており、その通信相手からのメッセージなどを受け取るために鍵生成を行うということである。

【0037】最初に鍵生成を行うときは、まずステップ204でディスプレイ111へ識別番号-識別名対応表124を表示する。次に、ステップ205で、操作員は該ディスプレイ111の表示を見て通信相手を選び、キーボード112より通信相手と自分の所属および名前を入力する。ここでは、操作員がA事業所のeさんであるものとし、eさんが本社のaさんおよびA事業所のcさんを通信相手に選び、それらの事業所識別番号と個人識別番号を入力したとする。さらに、自分の所属と名前であるA事業所のeを特定する事業所識別番号と個人識別番号も入力する。

【0038】次に、ステップ206で、該入力情報と識別番号-識別名対応表124を参照して、図4に示すような通信宛先情報を生成する。通信宛先情報は、事業所番号と配布リストを並べたものと乱数とからなる。事業所番号は2進の数値データ、配布リストは各ビットがその事業所の各個人に対応しているビットデータである。

【0039】図4において、事業所番号（事業所識別番号）401は2進数の数値データ「1」であることにより、事業所番号が「1」、すなわち本社が通信宛先の1つであることを示す。配布リスト402は、ビット列の下から第2ビット目がビット「1」であることにより、本社（事業所番号が「1」）の個人識別番号が「2」、すなわちaさんが通信宛先の1人であることを示す。同様に、事業所番号403は値「2」でA事業所が通信宛先の1つであり、その配布リスト404は個人識別番号が「1」と「3」、すなわちcさんとeさんがそれぞれ通信宛先の1人であることを示す。また、乱数405は本ステップ206の実施時点で新たに生成される乱数である。このような通信宛先情報を生成して、ICカード101に送信する。

【0040】次に、ステップ207でICカード101において図3に示す動作（後述するグループ鍵の生成）が実施される。その間、WS102側は待機する。ICカード101でのグループ鍵の生成が終了したら、ステップ208でICカード101から返される値であるグループ鍵を受け取り、メモリ114内のグループ鍵の記憶領域127に書き込む。そして、ステップ209で該通信宛先情報を（図4）を通信ボード108経由で通信網1

17に送信し、ステップ210で処理を終了する。以後、この端末では生成したグループ鍵を用いて通信メッセージを暗号化し送出する。また、相手から送られてきた通信メッセージは生成したグループ鍵を用いて解読する。

【0041】次に、最初に鍵を生成するのではないときは、まずステップ211でICカード101内のデータである事業所識別番号118と個人識別番号119をWS102内のメモリ114の領域125と126に書き込む。次に、ステップ212で通信網117から通信宛先情報が来るのを待機する。通信宛先情報が来たら次のステップへ進む。本例では、図4の通信宛先情報を受信するものとする。

【0042】ステップ213では、該通信宛先情報がメモリ114の事業所識別番号125と個人識別番号126で示される宛先を含んでいるかどうかを検査する。もし、含んでいればステップ214に進み、さもなければステップ218へ進み処理を終了する。

【0043】ステップ214では、該通信宛先情報をICカード101に送信する。そして、ステップ215でICカード101において図3に示す動作（後述するグループ鍵の生成）が実施される。その間、WS102側は待機する。ICカード101でのグループ鍵の生成が終了したら、ステップ216でICカード101から返される値であるグループ鍵を受け取り、メモリ114内のグループ鍵の記憶領域127に書き込む。そして、ステップ217で処理を終了する。以後、この端末では生成したグループ鍵を用いて、受け取った通信メッセージを解読する。また、相手に通信メッセージを送るときは、生成したグループ鍵を用いて暗号化し送出する。

【0044】図3は、メモリ104に格納されているグループ鍵生成プログラム1の動作を説明するためのフローチャートを示す。まずステップ301で処理が開始され、ステップ302でICカード側インターフェース105経由で通信宛先情報を（図4）を受信する。次に、ステップ303で該通信宛先情報に事業所識別番号118と個人識別番号119が同時に含まれるかどうかを検査する。もし、含まれていればステップ304へ進む。さもなければ、ステップ308へ進む。

【0045】いま図3の処理が実行されているICカードが図1のICカード101（A事業所のeさんのもの）であって、受け取った通信宛先情報が図4に示す数値例の場合は、事業所番号403の欄が数値「2」で、それに引き続配布リスト404の欄で第3ビット目にビット「1」が立っていることから、事業所識別番号118（数値は「2」）と個人識別番号119（数値は「3」）が同時に含まれていると判定される。

【0046】次に、ステップ304では、使用すべきマスク鍵の種類を図6に示す手順（後述する）で選定する。そして、ステップ305で該宛先通信情報を該マスク

タ鍵を使ってハッシュトータルを計算する。すなわち、 $H(K, M)$ (マスタ鍵、宛先通信情報)とする。ここに、 $H(K, M)$ はハッシュ関数であり、例えば、文献：宝木、「暗号方式と応用」、情報処理学会誌、1991年6月、で定義されたものなどを用いる。次に、ステップ306で該ハッシュトータルをICカード側インターフェース105経由でWS102に出力し、ステップ307で処理を終了する。このハッシュトータルがグループ鍵として用いられる。

【0047】一方、ステップ303で通信宛先情報に事業所識別番号118と個人識別番号119が同時に含まれていないときは、ステップ308で「拒否」通知をICカード側インターフェース105経由でWS102に出力し、ステップ309で処理を終了する。

【0048】図6は、図3の処理のうちのステップ304の詳細な動作を説明するためのフローチャートを示す。まず、ステップ601で処理が開始されると、ステップ602で通信宛先情報(図4)内の事業所番号のデータが1つだけかどうかを検査する。もし、1つだけならその事業所のみとの通信であるから、ステップ608へ進み、单一事業所用マスタ鍵120をメインルーチンへ返して、ステップ609へ進む。ステップ602で通信宛先情報(図4)内の事業所番号のデータが1つより多いときは、ステップ603へ進む。図4の数値例では事業所番号欄の数は2つ以上ある。

【0049】次に、ステップ603でメモリ103に記録されている部分域用マスタ鍵122, 123, …がすべて検査されたかどうかを判定する。もし、すべて検査されたのであれば、ステップ607へ進む。さもなければ、ステップ604へ進む。図5は、部分域用マスタ鍵のフォーマット例を示す。部分域用マスタ鍵は、事業所リスト501とそれに対するマスタ鍵情報502を備えている。事業所リスト501は、各事業所に対応するビットを並べたビットデータである。図5の例では、事業所リスト501の最下位ビット(第1ビット)が「1」、第2ビットが「1」で、他のビットは「0」であるから、このマスタ鍵情報502は事業所識別番号が「1」と「2」の事業所のグループの部分域用マスタ鍵であることとなる。

【0050】次に、ステップ604では、該部分域用マスタ鍵(図5)の事業所リスト501の欄が該通信宛先情報(図4)に示される事業所をすべて含むかどうかを検査する。もし、含まれていれば、ステップ606に進む。さもなければ、ステップ605に進む。図5の数値例では、事業所リスト501は事業所識別番号が「1」と「2」である。図4の数値例では事業所番号401は事業所「1」を、事業所番号403は事業所「2」を示している。図4においてその他の…の部分が空白であれば、部分域用マスタ鍵(図5)の事業所リスト(501)の欄は該通信宛先情報(図4)に示される事業所を

すべて含むことになる。

【0051】ステップ604で部分域用マスタ鍵の事業所リスト501の欄が通信宛先情報に示される事業所をすべて含むのではない場合は、ステップ605でメモリ103上の次の部分域用マスタ鍵を設定する。そして、ステップ603へ戻る。

【0052】ステップ604で部分域用マスタ鍵の事業所リスト501の欄が通信宛先情報に示される事業所をすべて含む場合は、ステップ606で該部分域用マスタ鍵(図1の部分域用マスタ鍵122, 123, …のうちの1つ)をメインルーチンへ渡す。そして、ステップ609へ進む。

【0053】ステップ603で部分域用マスタ鍵をすべて調べた場合は、ステップ607で全域用マスタ鍵121をメインルーチンへ渡す。そして、ステップ609へ進む。ステップ609で処理を終了する。

【0054】上述したように、单一事業所用マスタ鍵120は、同じ事業所に属するICカードではすべて同じ値が書かれている。例えば、A事業所のcさん、dさん、およびeさんのICカードの单一事業所用マスタ鍵120はすべて同じ値である。また、全域用マスタ鍵121は、事業所が同じかどうかにかかわらずすべてのICカードで同じ値である。部分域用マスタ鍵122, 123…は、事業所リスト(図5の501)で指定される事業所に属すICカードはすべて同じ値である。例えば、図5の501の例は、事業所番号「1」と「2」すなわち、本社とA事業所に属するICカードに記録されるものである。

【0055】以上より、本実施例によれば、ディスプレイ112に表示される事業所別識別名一覧表124を見て通信相手を選定しキーボードを入力することにより、ICカード101で自分および通信相手に共通に保持されるグループ鍵が生成され、WS102のメモリ114にそのグループ鍵が設定される。つまり、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。

【0056】また、グループ鍵を計算するうえで、グループ鍵←H (マスタ鍵、通信宛先情報) (ただし、Hはハッシュ関数)

の計算式で使用されるマスタ鍵は、ICカード101に入力される通信宛先情報(図4)の数値データによって異なる。例えば、図4に記入された数値例の場合、もし図の…の部分が空白であれば、図5の数値例に示されるような部分域用マスタ鍵が使用される。この部分域用マスタ鍵は、事業所番号「1」と「2」、すなわち本社とA事業所に属するICカードにしか入っていない数値データである。これにより、他の事業所に属するICカードの中身が万一漏洩したとしても本マスタ鍵は含まれないので、本事業所番号「1」と「2」の間の通信の安全

性に影響を与えることはない。

【0057】複数事業所にまたがり鍵共有を行おうとする場合に、もし適当な部分域用マスタ鍵がICカード内になかったとする。このときは、全域用マスタ鍵が使われ、グループ鍵が生成される。各ICカードには、全域用マスタ鍵のほかに単一事業所用マスタ鍵や幾つかの部分域用マスタ鍵が含まれている。したがって、例えば1枚のICカードの中身が漏洩したとすると全域用マスタ鍵が知られてしまうので、その場合の安全性は低下するが、すべてのICカードの中身が漏洩していない限り、グループ間の通信においては安全性が高い。指定された通信相手のICカード以外ではグループ鍵は生成されないからである。

【0058】(実施例の変形例1)前記の実施例では、ICカード101内のマスタ鍵120, 121, 122, 123, …は、予め設定されているとした。この代わり、図7に示すように、ICカード101内のメモリ103に予めICカード個別の個人鍵701を設定しておく、各個人鍵を集中管理する鍵センタからマスタ鍵120, 121, 122, 123, …をICカード別に個人鍵701で暗号化しマスタ鍵暗号文として送信し、受信側のICカード内の暗号関数702でそのマスタ鍵暗号文を復号化してメモリ103内に設定するようにしてもよい。

【0059】この変形例1により、マスタ鍵漏洩等の事情でマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。

【0060】(実施例の変形例2)前記の実施例では、ICカード101内のマスタ鍵120, 121, 122, 123, …は、予め設定されているとした。この代わり、図8に示すように予めICカード個別に第1のセンタに登録されている個人鍵801、第2のセンタに登録されている個人鍵802、…を設定しておく。各センタは、ICカードの鍵を集中管理する。マスタ鍵更新時には、第1のセンタから、マスタ鍵情報を生成するために用いる第1のマスタ鍵登録情報を個人鍵801で暗号化しマスタ鍵分割暗号文として送信する。受信側のICカードでは、暗号関数702でこのマスタ鍵分割暗号文を復号化し、第1のマスタ鍵登録情報を得る。同様に、第2のセンタから、第2のマスタ鍵登録情報を個人鍵802で暗号化して送信し、受信側のICカード内の暗号関数702で復号化し、第2のマスタ鍵登録情報を得る。他のセンタがある場合は、同様にしてマスタ鍵登録情報を得る。そして、ICカード101内で、マスタ鍵←第1のマスタ鍵登録情報+第2のマスタ鍵登録情報+…

(ただし「+」はビット毎の排他的論理和とする)の計算式でマスタ鍵を計算して、メモリ103内に設定するようにしてもよい。

【0061】この変形例2によれば、マスタ鍵は複数の鍵センタの共同作業により生成される。したがって、複数の鍵センタが結託しない限り、マスタ鍵がセンタに知られることはない。

05 【0062】(実施例の変形例3)前記の実施例では、図4に示すように通信宛先情報の最後の欄405を乱数としていたが、乱数ではなく時間の経過とともに異なるような時間情報やシーケンス番号等にしてもよい。

【0063】

10 【発明の効果】以上説明したように、本発明によれば、複数事業所にまたがり好みの複数人の通信相手を指定して、グループ暗号通信を行うためのグループ鍵を共有することができる。また、通信中の事業所以外の事業所に属するICカードの中身が万一漏洩したとしても、該事業所の間の通信の安全性に影響を与えることはない。

15 【0064】さらに、複数事業所にまたがり鍵共有を行おうとする場合、もし適当な部分域用マスタ鍵がICカード内になかったときには、全域用マスタ鍵が使われ、グループ鍵が生成される。この場合でも、すべてのICカードの中身が漏洩していないければ、安全である。

20 【0065】個人鍵などを用いれば、マスタ鍵漏洩等の事情によりマスタ鍵を更新する必要が生じた場合に、電話確認後個別暗号通信等の比較的安全な手段によりマスタ鍵を更新することが可能になる。さらに、マスタ鍵が複数の鍵センタの共同作業により生成されるようにして、複数の鍵センタが結託しない限りマスタ鍵が鍵センタの単独作業により知られることがないようにできる。したがって、通信当事者間のプライバシーを鍵センタに対して保護することができる。

30 【図面の簡単な説明】

【図1】本発明の第1の実施例である通信システムにおける端末の構成図を示す。

【図2】図1におけるグループ鍵生成プログラム2の動作フローチャートを示す。

35 【図3】図1におけるグループ鍵生成プログラム1の動作フローチャートを示す。

【図4】図1におけるICカード101に入力される通信宛先情報のフォーマット、および数値データ例を示す図である。

40 【図5】図1における部分域用マスタ鍵122, 123, …のフォーマット、および数値データ例を示す図である。

【図6】図3の処理のうちのステップ304の詳細な動作フローチャートを示す。

45 【図7】実施例の変形例1のシステム構成図を示す。

【図8】実施例の変形例2のシステム構成図を示す。

【図9】従来例のシステム構成図を示す。

【図10】本発明の第1の実施例である通信システムの構成図を示す。

50 【符号の説明】

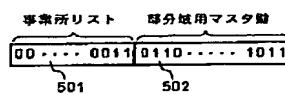
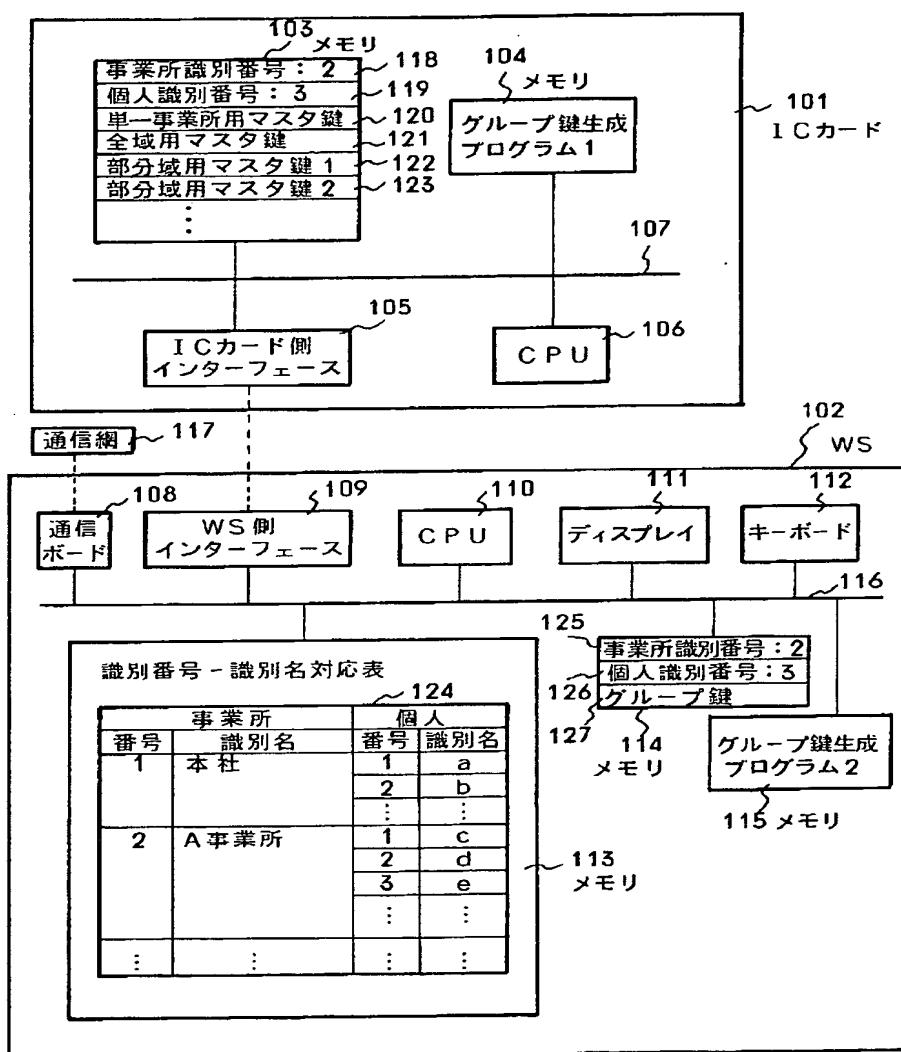
1001…通信網、1002, 1004, 1006, 1008, 1010…通信端末、1003, 1005, 1007, 1009, 1011…ICカード、1012, 1016, 1019, 1023, 1026…個別数値、1013, 1017…本社用マスタ鍵、1020, 1024, 1027…A事業所用マスタ鍵、1015, 1018, 1022, 1025, 1029…全域用マスター鍵、101…ICカード、102…ワークステーション(WS)、103, 104, 113, 114, 115…メモリ、106, 110…CPU、117…通信網。

【図1】

図 1

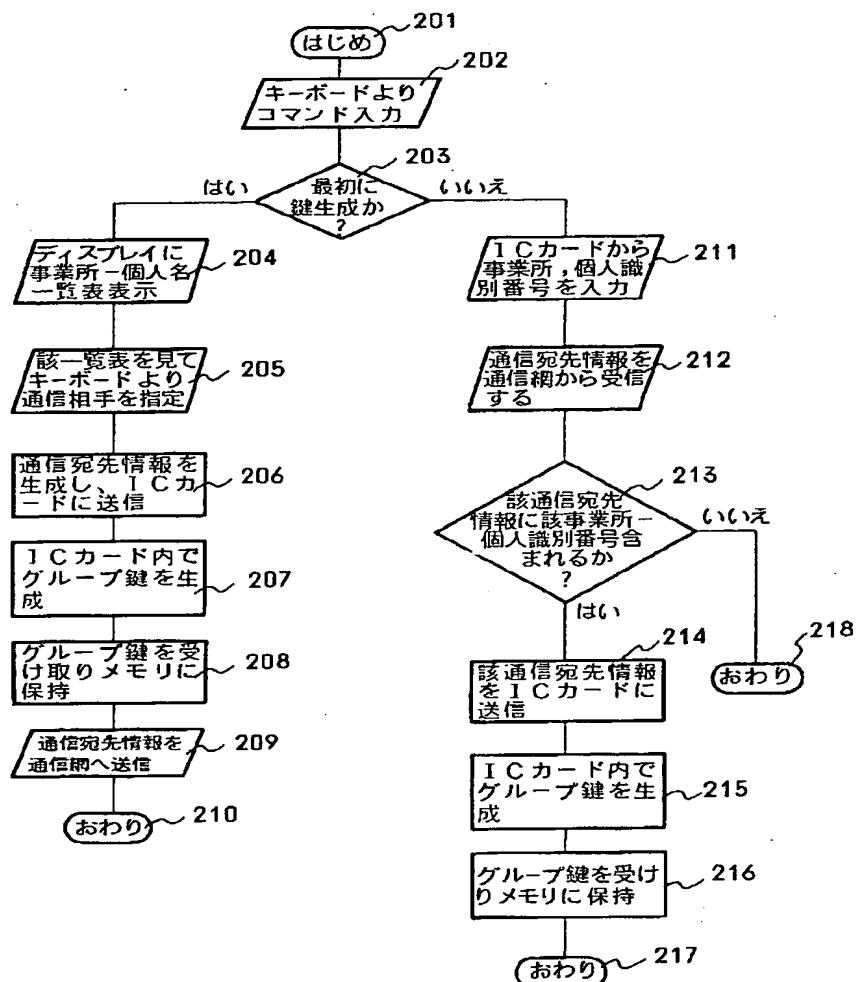
【図5】

図 5



【図2】

図 2



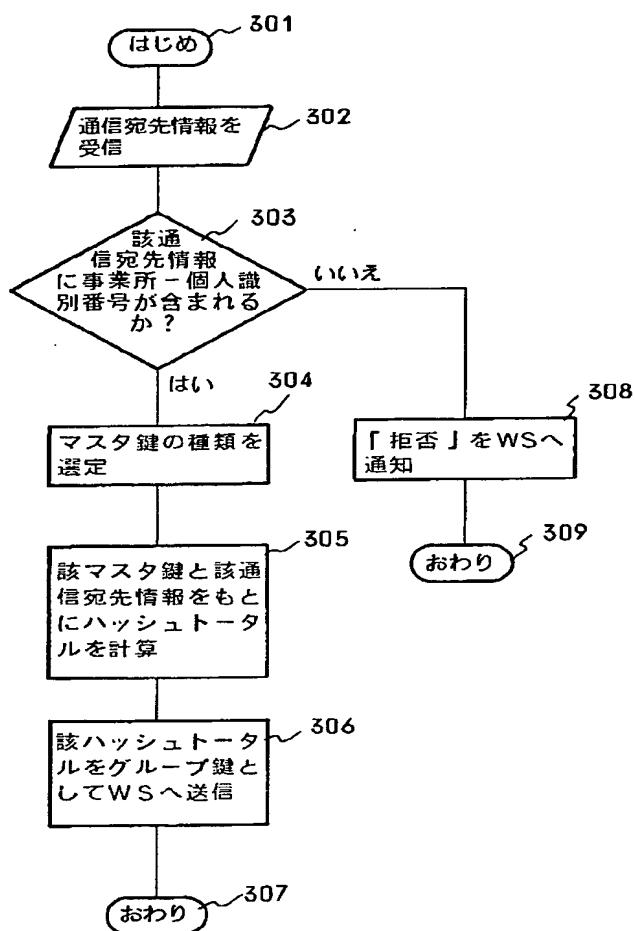
【図4】

図 4



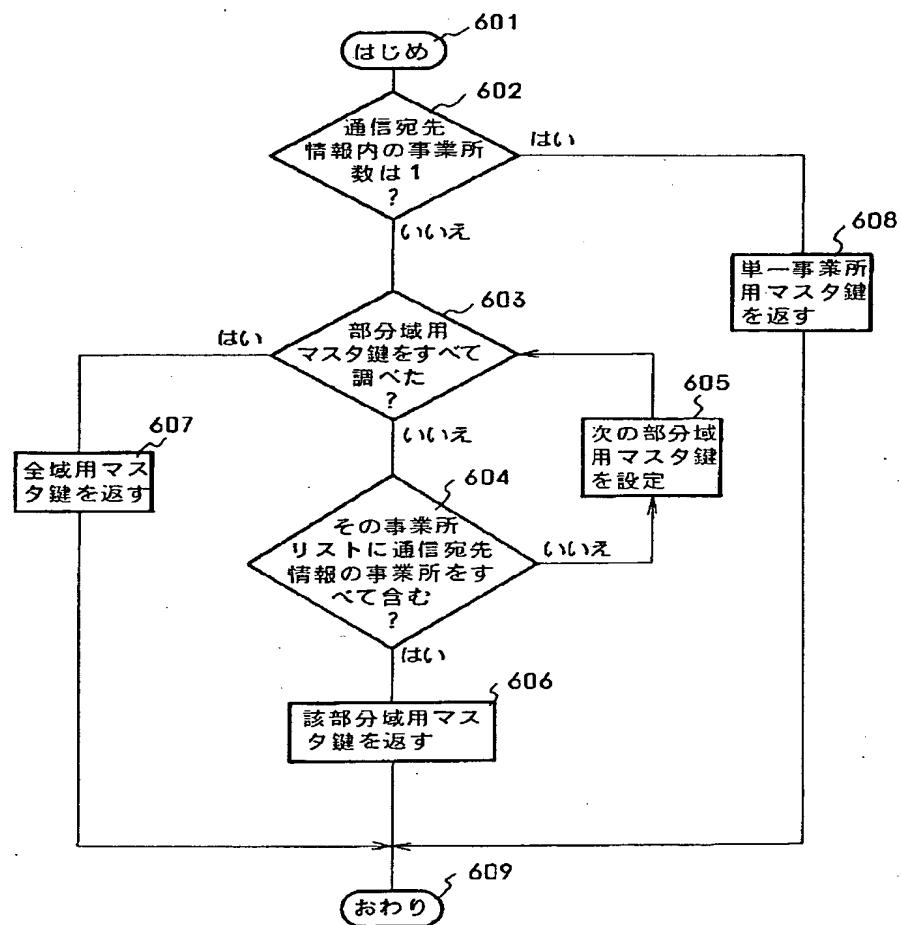
【図3】

図 3



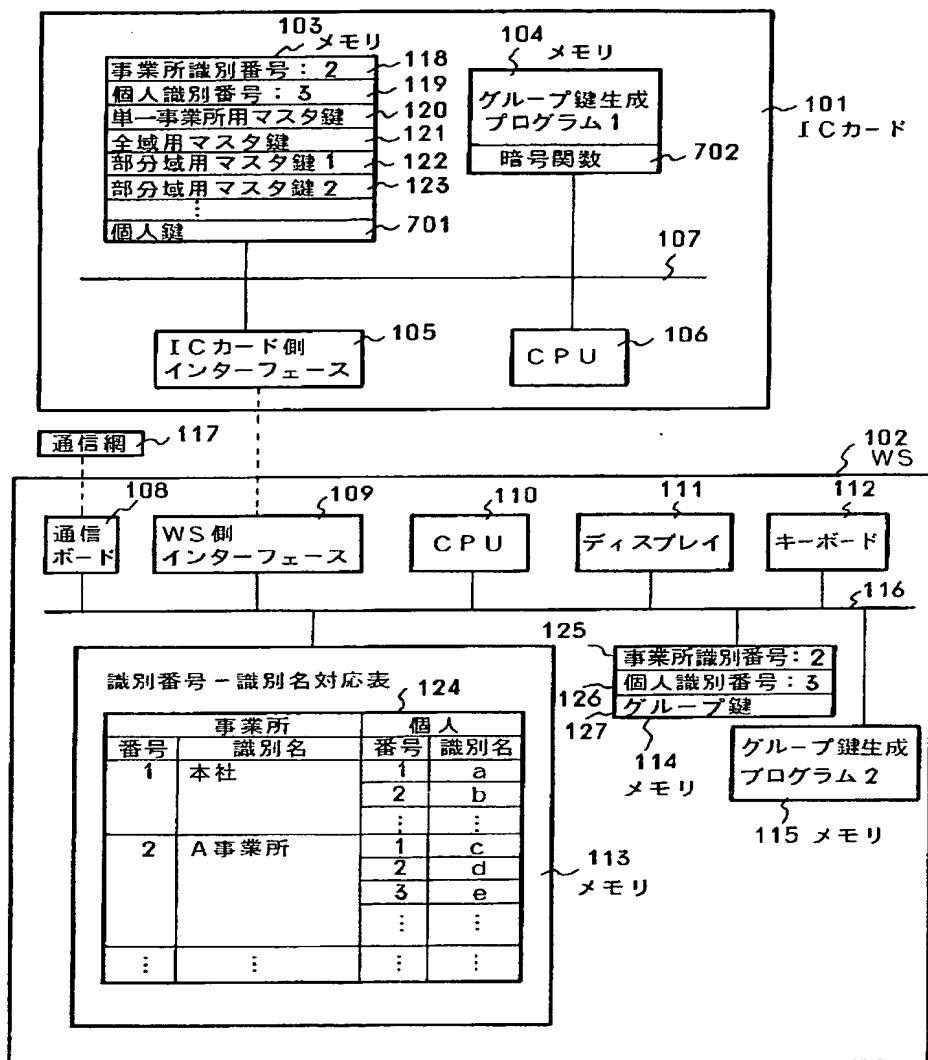
【図6】

図 6



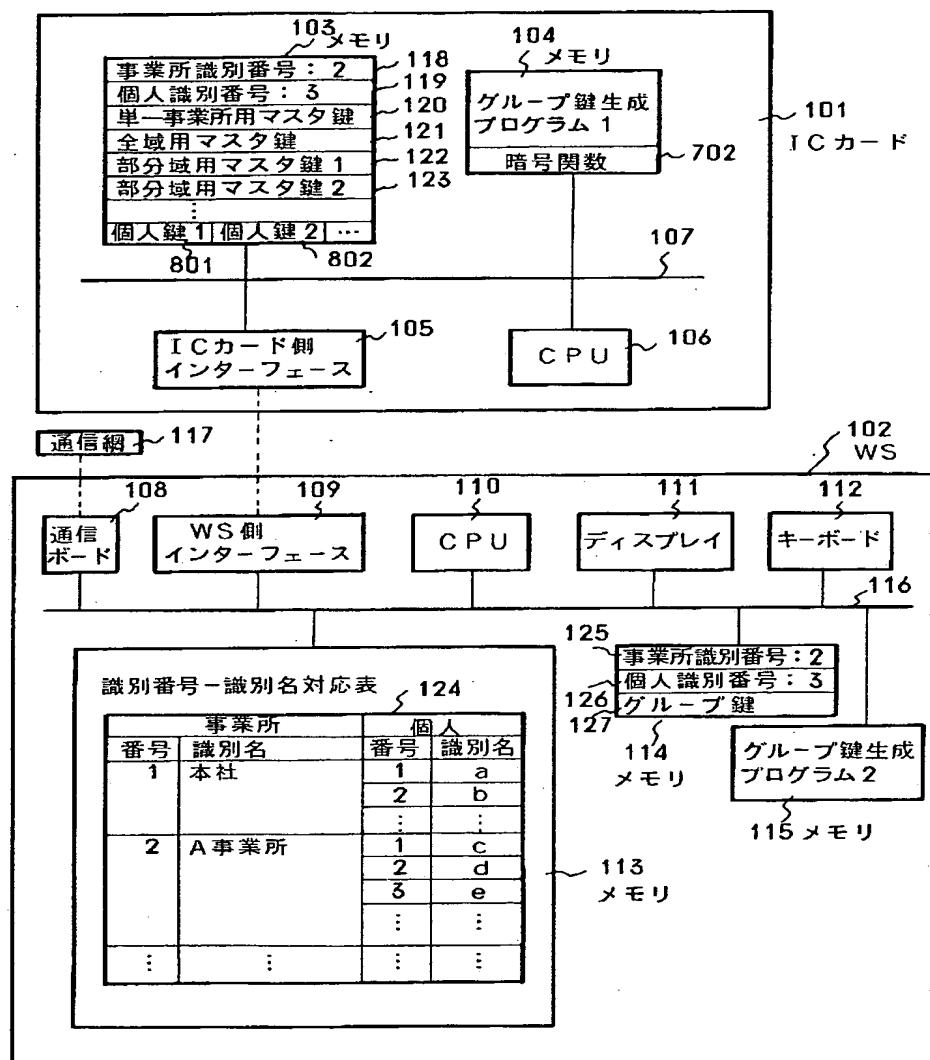
【図7】

図 7



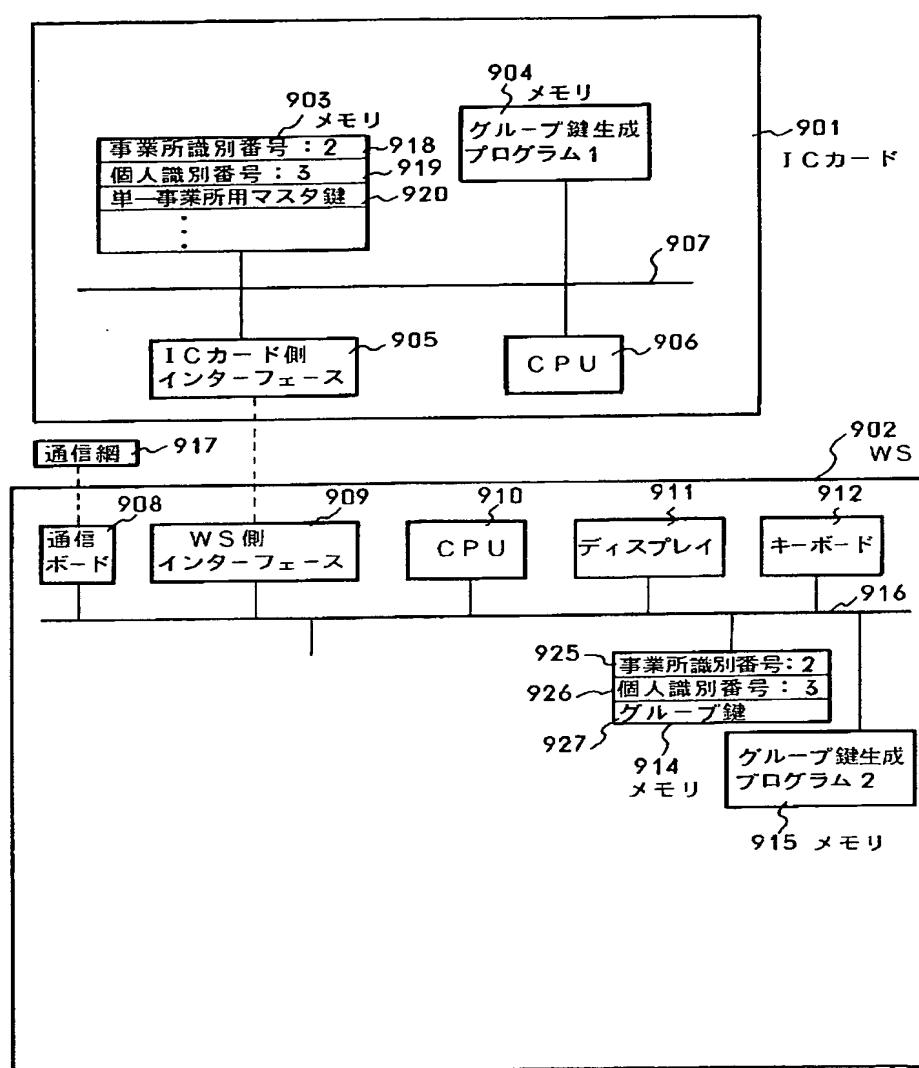
【図8】

図 8



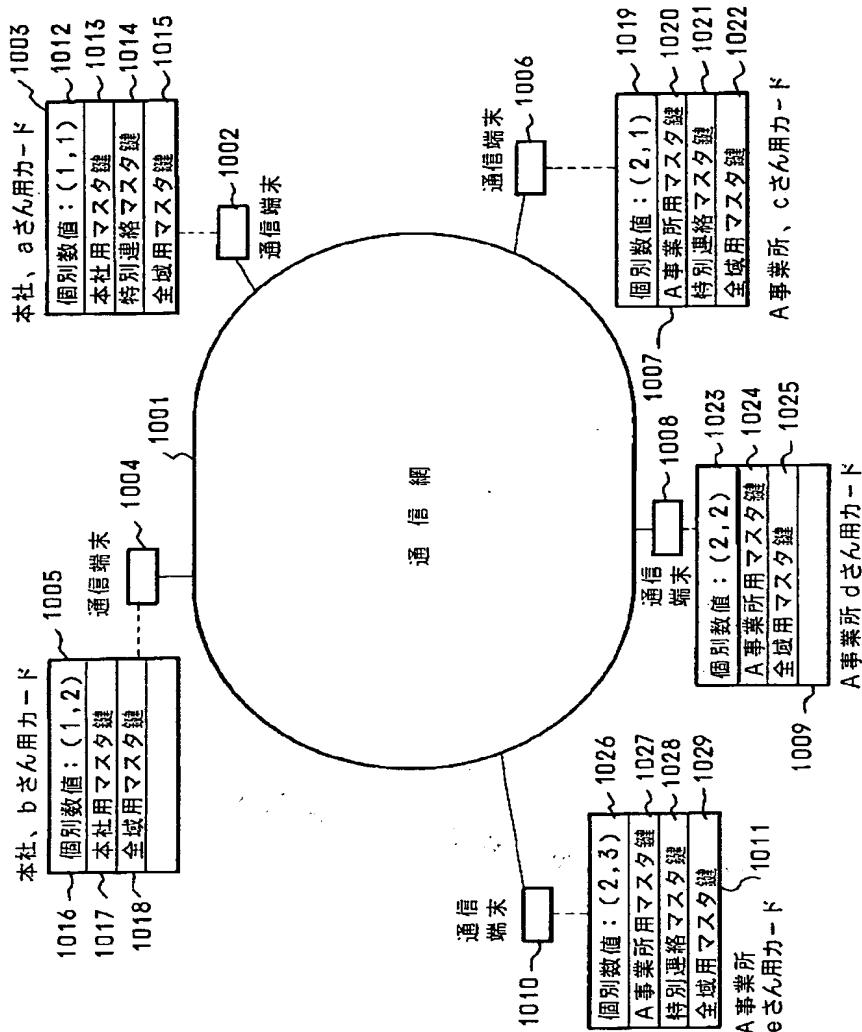
【図9】

図 9



【図10】

図 10



フロントページの続き

(72)発明者 松本 浩

愛知県名古屋市中区栄三丁目10番22号 日 45
立中部ソフトウェア株式会社内

(72)発明者 中村 勤

神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

This Page Blank (uspto)